

Blockchain-Enabled Multimodal Biometric Authentication for Secure E-Examinations: A Systematic Literature Review And ISDT-Oriented Design Research Agenda

Martin Mirianki Muriki¹, Dr. Paul Abuonji², Dr. Edwin Omol³

^{1,2,3}*School of Technology, KCA University, Kenya*

Abstract—The rapid expansion of electronic examination (e-examination) has shifted candidate identity verification and examination-record assurance from predominantly physical processes to information-system controls. Existing research has investigated biometric authentication, multimodal fusion, blockchain-based record management, remote proctoring, and privacy protection, but these streams have largely evolved independently. This paper develops a systematic-review framework and ISDT-oriented synthesis for explaining how complementary security capabilities should be integrated rather than treating blockchain and biometrics as interchangeable security technologies. The review is structured around PRISMA 2020 and PRISMA-S principles and uses four independent evidence streams covering e-examination security, multimodal biometrics, blockchain in education, and blockchain-biometric identity systems. Eligibility, screening, quality appraisal, structured extraction, descriptive synthesis, and thematic coding are explicitly specified to minimise technology-coupling bias and improve reproducibility. The synthesis distinguishes identity assurance from information integrity: multimodal biometrics primarily addresses candidate identity, whereas permissioned blockchain primarily provides tamper-evident auditability of authentication and examination events. The analysis further identifies a recurring tension between stronger identity assurance and the increased collection of sensitive biometric information, making privacy-preserving data separation a core architectural requirement. On this basis, the paper derives review-oriented design requirements covering multimodal identity assurance, transparent fusion, continuous assurance, privacy-preserving storage, tamper-evident logging, permissioned governance, interoperability, human-centred trust, and dual technical-behavioural evaluation. Rather than claiming that these requirements constitute an already validated design theory, the paper positions them as

evidence-derived inputs for subsequent Design Science Research. The resulting ISDT-oriented research agenda specifies how future artefact development can generate and empirically validate reusable design principles and testable propositions for secure, trustworthy, and privacy-preserving e-examination systems.

Index Terms—e-examination, electronic assessment, multimodal biometrics, blockchain, biometric authentication, privacy-preserving authentication, Information Systems Design Theory, Design Science Research, academic integrity, higher education.

I. INTRODUCTION

Electronic examination systems have become an important component of digital higher education because they support automated scheduling, electronic question delivery, rapid grading, flexible assessment delivery, and digital record management. However, moving assessment from controlled physical environments into distributed or remote information systems changes the security problem. Physical invigilation is replaced by software-mediated identity verification, monitoring, access control, and digital evidence management. The resulting problem is socio-technical: candidate impersonation, credential compromise, presentation attacks, examination fraud, record manipulation, privacy risks, and institutional trust can interact rather than occur independently. Biometric authentication addresses the identity-assurance side of this problem. Multimodal systems combine complementary biometric characteristics and can reduce dependence on a single modality. Recent work on multimodal authentication has also emphasised template protection and privacy criteria

such as irreversibility, unlikability, and revocability. However, a biometric system by itself does not establish an immutable record of the authentication event. Blockchain addresses a different problem by providing cryptographically linked, auditable and tamper-evident transaction records. Educational blockchain reviews have documented applications in credentials, records and other institutional processes, but the literature does not automatically establish how blockchain should interact with biometric identity verification in high-stakes assessment.

The central argument of this review is therefore that secure e-examination should be analysed as an integration problem. Biometrics and blockchain are complementary: the former contribute evidence about who is being authenticated, while the latter contributes evidence about the integrity and traceability of recorded events. This distinction also exposes a privacy challenge. Biometric information is sensitive and difficult to revoke if compromised, while immutable ledgers are intentionally resistant to modification. A secure architecture must consequently separate biometric information from ledger evidence and minimise what is permanently recorded.

A. Research Problem

Existing literature provides substantial technical knowledge about biometric recognition and blockchain-based integrity mechanisms, but comparatively less transferable design knowledge explains how the two capabilities should be combined within a socio-technical e-examination Information System. The problem is therefore not simply that existing examinations lack security technology. The problem is that the design relationships among identity assurance, record integrity, privacy, governance, usability, and trust remain insufficiently articulated.

B. Research Questions

RQ	Research question
RQ1	What security, authentication and integrity challenges are reported in e-examination systems?
RQ2	What biometric modalities and fusion approaches are used for candidate identity assurance?
RQ3	How is blockchain used to support examination, identity and educational-record integrity?

RQ4	How have blockchain and biometric authentication been integrated, and what technical architectures and evaluation strategies have been reported?
RQ5	What privacy, trust, governance, interoperability and usability issues constrain integrated approaches?
RQ6	What review-derived design requirements and research propositions can guide an ISDT-oriented Design Science Research programme?

C. Contributions

The paper makes five bounded contributions:

- 1) A reproducible four-stream systematic-review protocol aligned with PRISMA 2020 and PRISMA-S;
- 2) A technology taxonomy distinguishing identity assurance, information integrity, and integrated blockchain-biometric functions;
- 3) A privacy-preserving architectural synthesis separating biometric data from blockchain evidence;
- 4) A set of review-derived design requirements that are explicitly distinguished from empirically validated ISDT principles; and
- 5) An ISDT-oriented research agenda linking requirements, artefact development, technical evaluation, behavioural evaluation, and subsequent theory validation.

II. CONCEPTUAL AND THEORETICAL FOUNDATIONS

A. E-Examination Security as a Socio-Technical Problem

E-examination security extends beyond login authentication. A trustworthy assessment environment must establish candidate identity, preserve identity assurance during relevant parts of the examination, protect examination content and personal information, and preserve evidence about examination events. Research on digital proctoring demonstrates that monitoring and authentication technologies can introduce privacy, fairness and security concerns of their own.

Accordingly, examination integrity should be treated as a multi-dimensional information-system property rather than a single authentication metric.

B. Multimodal Biometric Authentication

Biometric authentication uses physiological or behavioural characteristics to establish identity. Fingerprint, facial and voice recognition are particularly relevant to remote assessment because they can be acquired using commonly available devices or established sensors.

Unimodal systems, however, remain sensitive to modality-specific failure modes, including environmental variation, sensor quality, occlusion, spoofing and intra-user variability. Multimodal authentication combines evidence from two or more modalities and can compensate for some individual weaknesses.

Fusion can occur at sensor, feature, score, rank or decision level. Score-level fusion is attractive for an integrated Information System because modality-specific matchers can remain independently optimised while their outputs are normalised and combined. However, improved recognition performance does not eliminate privacy risk. Template protection must address irreversibility, unlinkability and revocability, and the architecture must minimise the exposure of biometric information.

C. Blockchain for Examination Integrity

Blockchain is relevant to e-examination because it can provide tamper-evident records, distributed verification among authorised participants, cryptographic integrity and traceability. Educational blockchain reviews have identified credentials, records and other institutional processes as major application areas.

For examination systems, the most defensible role of a permissioned blockchain is therefore not to store raw biometric data but to preserve evidence that an authentication or examination event occurred and that its recorded representation has not been altered.

D. Information Systems Design Theory

Information Systems Design Theory provides the theoretical lens for converting technological capabilities into prescriptive design knowledge. Gregor and Jones identify eight components of a

design theory: purpose and scope, constructs, principles of form and function, artefact mutability, testable propositions, justificatory knowledge, principles of implementation, and expository instantiation.

This structure is appropriate because the objective is not merely to propose a software architecture but to explain why particular design configurations should produce desired organisational outcomes and under what conditions.

E. Design Science Research

Design Science Research provides the methodological pathway through which the design knowledge can later be instantiated and evaluated. Peffers et al. specify problem identification, objectives, design and development, demonstration, evaluation, and communication as core activities.

Hevner et al. emphasise relevance, rigor and evaluation, while Gregor and Hevner distinguish different forms of DSR knowledge contribution. The present review therefore treats DSR as the future artefact-development methodology and ISDT as the theoretical structure for expressing the resulting design knowledge.

III. SYSTEMATIC LITERATURE REVIEW METHODOLOGY

The review protocol is designed to be reproducible and to avoid a major weakness of tightly coupled searches: requiring a paper to contain e-examination, biometrics and blockchain simultaneously can exclude relevant evidence from adjacent technological streams. Accordingly, the review uses four independent search streams that are integrated during synthesis rather than at retrieval.

A. Review Reporting Framework

The review follows PRISMA 2020 for reporting the review process and PRISMA-S for transparent reporting of literature-search methods.

PRISMA-S specifically addresses the reproducibility of database searching, including information sources, search strategies and search-management procedures.

B. Information Sources

Source	Purpose	Search treatment
Scopus	Broad multidisciplinary coverage	Database-specific syntax; title/abstract/keyword
Web of Science Core Collection	Citation-indexed multidisciplinary coverage	Topic search and cited-reference expansion
IEEE Xplore	Engineering and computing literature	Metadata/full-text search where available
ACM Digital Library	Computing and information-systems research	Abstract/keyword/full-text search
ScienceDirect	Elsevier journals and conference literature	Title/abstract/keyword search
SpringerLink	Computing, security and education literature	Keyword and metadata search
Wiley Online Library	Information systems and security literature	Keyword search
Taylor & Francis Online	Education and information-systems literature	Keyword search

The final manuscript must report the exact date, record count for every source. Those values are intentionally not fabricated in this version.

C. Four-Stream Search Strategy

Stream	Core search logic	Purpose
A	(e-examination OR electronic examination OR online examination OR digital assessment OR remote examination) AND (security OR authentication OR identity OR impersonation OR academic integrity)	Capture examination-security evidence
B	(biometric* OR multimodal biometric* OR biometric authentication) AND (face OR facial OR fingerprint OR voice OR iris) AND (authentication OR verification OR identification)	Capture biometric evidence
C	(Blockchain OR distributed ledger OR smart contract* OR permissioned blockchain) AND (education OR university OR higher education OR examination OR assessment OR credential*) AND (security OR integrity OR trust OR privacy OR audit*)	Capture educational blockchain evidence
D	(Blockchain OR distributed ledger OR smart contract*) AND (biometric* OR multimodal biometric* OR digital identity OR authentication) AND (security OR privacy OR trust OR integrity)	Capture integrated identity evidence

D. Eligibility Criteria

Include	Exclude
Peer-reviewed journal or high-quality scholarly conference study	Editorials, opinion pieces, news, marketing material
Study addresses one or more review streams	Studies unrelated to authentication, examination security, biometrics or blockchain
Reports sufficient methods and findings for extraction	Abstract-only records where full text cannot be assessed
Published within the defined review period, with seminal methodological/theoretical sources retained where justified	Duplicate publication records
English-language study if language restriction is imposed and documented	Pure cryptocurrency/financial studies without relevant identity, education or security implications

E. Screening and Inter-Reviewer Procedure

Two-stage screening should be performed: title/abstract screening followed by full-text eligibility assessment. At least two reviewers should

independently assess a predefined sample of records, with disagreements resolved through discussion or a third reviewer. Inter-reviewer agreement should be reported using percentage agreement and, where

appropriate, Cohen's kappa. The screening log should preserve exclusion reasons at full-text stage. The final

PRISMA flow diagram must be generated directly from this log.

F. Quality Appraisal

Domain	Question	Scoring
Research objective	Is the research question/objective explicit?	0–2
Method transparency	Are design, dataset/sample and procedures sufficiently described?	0–2
Evaluation rigour	Are evaluation procedures and metrics justified?	0–2
Threats/limitations	Are validity threats or limitations acknowledged?	0–2
Reproducibility	Are sufficient implementation/search details provided?	0–2
Theoretical grounding	Is the study linked to a coherent conceptual/theoretical basis?	0–2

A study-level quality score should be used for sensitivity analysis rather than as an arbitrary

exclusion mechanism unless the protocol specifies a threshold in advance.

G. Data Extraction and Coding

Category	Variables
Bibliographic	Author, year, venue, DOI, country, database
Technology	Biometric modality, fusion level, blockchain architecture, platform
Security	Authentication, spoofing resistance, integrity, access control
Privacy	Template protection, encryption, off-chain storage, minimisation, retention
Evaluation	FAR, FRR, EER, accuracy, latency, throughput, usability, trust
Organisation	Governance, interoperability, scalability, stakeholder acceptance
Theory	ISDT, DSR, UTAUT, security models, trust theories
Evidence quality	Quality score, study limitations, external-validity indicators

H. Synthesis Strategy

Because the expected studies are heterogeneous in population, technology, evaluation metrics and research design, statistical meta-analysis should not be assumed.

Descriptive synthesis will quantify study characteristics where the extraction dataset supports aggregation.

Thematic synthesis will identify recurring technical, privacy, trust, governance and design patterns.

Where multiple studies report comparable biometric metrics under comparable datasets and protocols, effect-size synthesis may be considered; otherwise, the paper will explicitly justify why meta-analysis is inappropriate.

Figure 1. PRISMA 2020 Evidence-Gated Flow Diagram

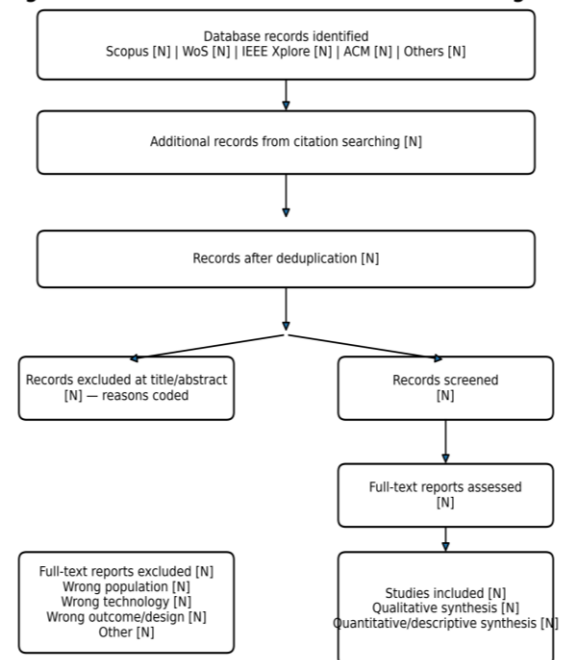
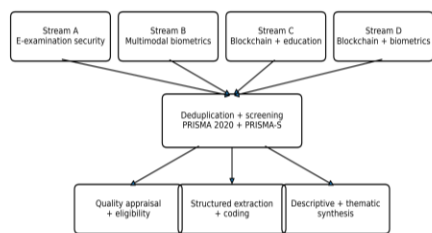


Fig. 1. PRISMA 2020 evidence-gated flow diagram. Numerical fields are populated only from the verified search and screening dataset.

Figure 2. Four-Stream Search Architecture Designed to Minimise Technology-Coupling Bias



The streams are searched independently and synthesised at the evidence-integration stage.

Fig. 2. Four-stream search architecture used to reduce technology-coupling bias.

IV. EVIDENCE SYNTHESIS

The evidence synthesis is organised around the distinction between identity assurance and information integrity. This prevents a common conceptual error in the literature: treating blockchain as if it independently authenticates a candidate. Blockchain can preserve the integrity of a transaction representing an authentication event, but the correctness of that underlying event depends on the authentication mechanism.

A. Identity Assurance

Biometric evidence indicates that multimodal systems can provide stronger identity assurance than single modalities by combining complementary evidence. The advantage is conditional rather than absolute: environmental variation, presentation attacks, template compromise, algorithmic error and modality correlation remain relevant. Consequently, multimodal design should be accompanied by liveness or presentation-attack detection, calibrated thresholds, failure handling and protected templates.

B. Examination-Record Integrity

Blockchain evidence supports a complementary role in preserving auditability and tamper evidence. Permissioned architectures are particularly relevant to universities because institutional participants can be governed through membership rules, access policies and controlled consensus. However, immutability

does not make an incorrect input correct. If a fraudulent authentication event is accepted before it is written to the ledger, blockchain can preserve the fraudulent event rather than prevent it.

C. Technical Evaluation Gap

Technical evaluation in the reviewed domain is expected to be dominated by authentication accuracy, FAR, FRR, EER and computational performance. Blockchain studies commonly emphasise latency, throughput, transaction integrity and scalability. A stronger integrated evaluation must test the complete chain from biometric acquisition to authentication decision and audit-record generation. It should compare the proposed architecture against a baseline, isolate the contribution of multimodal fusion, and separately measure ledger overhead.

D. Privacy and Data-Protection Gap

Privacy is not a secondary constraint. Biometric characteristics are sensitive because they are closely associated with identity and are difficult to replace after compromise. The combination of biometrics with an immutable ledger therefore creates a design tension: the ledger should provide durable integrity evidence while the biometric information should remain subject to minimisation, access control, retention and deletion policies.

E. Trust, Governance and Acceptance

Trust should not be equated with cryptographic integrity. Stakeholders may trust a system only when its security claims are understandable, its privacy practices are proportionate, its governance is accountable, and its operation is usable. Consequently, technical metrics alone cannot establish organisational trustworthiness. Behavioural evaluation should examine perceived usefulness, effort expectancy, trust, privacy assurance, usability and behavioural intention using validated instruments where applicable.

V. CROSS-DOMAIN EVIDENCE SYNTHESIS

Dimension	Biometrics	Blockchain	Integrated systems	Design implication
Identity assurance	Primary capability	Indirect	Primary integration need	Multimodal verification + liveness
Record integrity	Limited	Primary capability	Strong complement	Hash-based event anchoring

Privacy	Template/data risk	Immutability tension	High sensitivity design	Off-chain protected biometric data
Trust	Accuracy can support confidence	Integrity/auditability can support confidence	Requires socio-technical alignment	Transparent governance + evidence
Governance	Algorithm/sensor governance	Membership/consensus governance	Cross-layer governance	Permissioned participation
Interoperability	Sensor/algorithm heterogeneity	API/data/ledger heterogeneity	High complexity	Standardised interfaces
Scalability	Inference/processing cost	Consensus/transaction cost	Combined overhead	Benchmark concurrent users
IS design knowledge	Often algorithmic	Often architectural	Limited prescriptive synthesis	ISDT-oriented principles

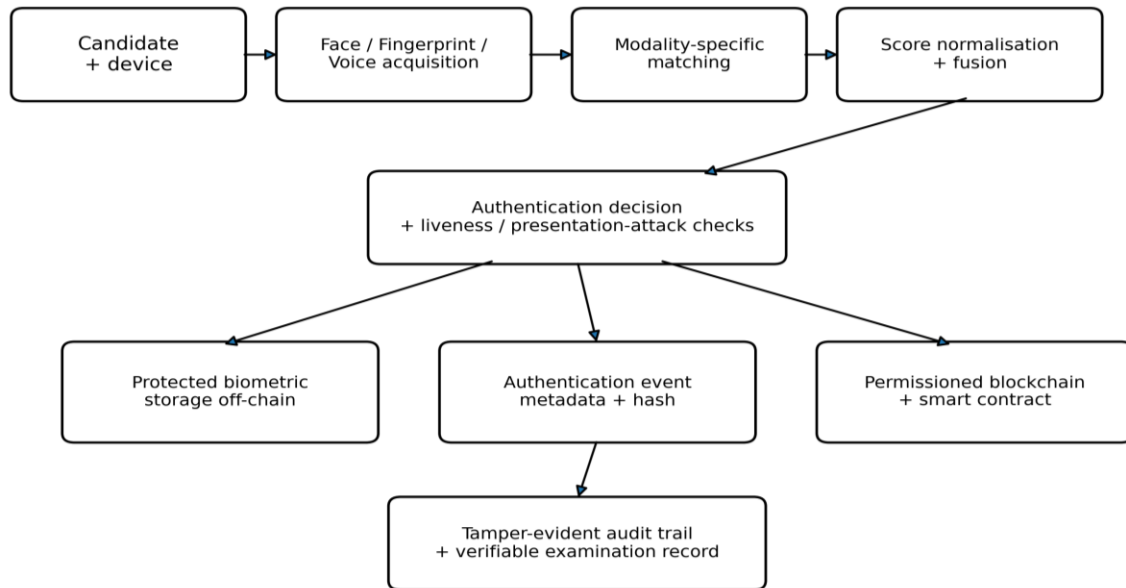


Fig. 3. Privacy-preserving technical architecture linking multimodal biometric identity assurance with permissioned blockchain auditability.

Figure 4. Threat-to-Control Mapping for the Integrated Architecture

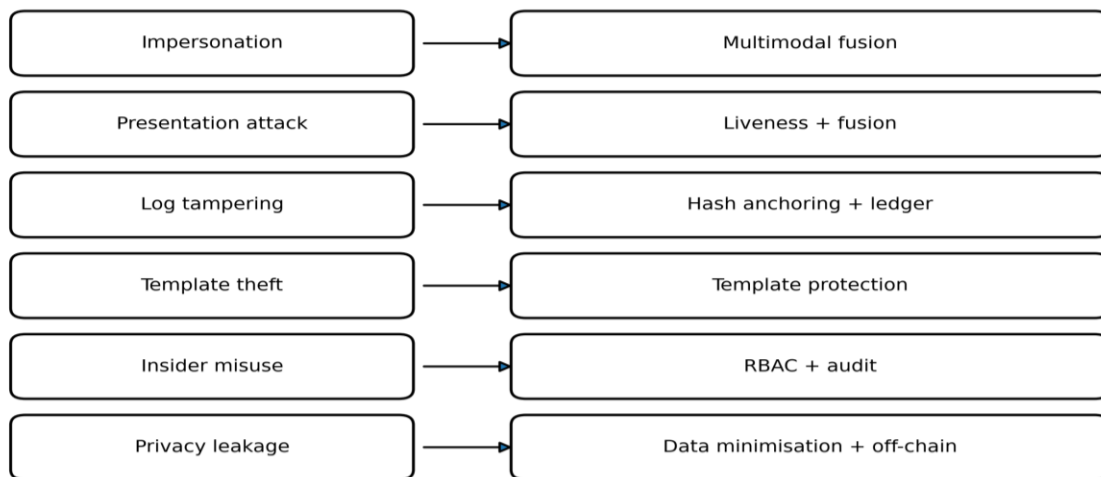


Fig. 4. Threat-to-control mapping for the integrated architecture.



Principle: raw biometric information is not written to the blockchain; only the minimum integrity evidence required for auditability is anchored.

Fig. 5. Privacy-by-design lifecycle for biometric examination data.

VI. REVIEW-DERIVED DESIGN REQUIREMENTS

The following requirements are derived as review-level design requirements. They are not presented as

empirically validated ISDT principles. Validation belongs to the subsequent Design Science Research phase.

ID	Requirement	Design statement
DR1	Multimodal identity assurance	The system should combine at least two complementary biometric modalities to reduce dependence on a single identity signal.
DR2	Transparent fusion	The fusion mechanism should be explicit, calibratable and auditable, with modality-level scores retained where necessary for diagnostics.
DR3	Continuous/risk-adaptive assurance	Identity assurance should not be limited to initial login where the threat model requires continuing verification.
DR4	Presentation-attack resistance	Biometric authentication should incorporate liveness or other presentation-attack controls appropriate to the modalities.
DR5	Privacy-preserving data separation	Raw biometric information and reconstructable templates should remain off-chain; the ledger should contain minimum integrity metadata.
DR6	Tamper-evident event logging	Authentication and examination events should generate cryptographically verifiable records.
DR7	Permissioned governance	Ledger participation, smart-contract execution and access should be governed through institutional roles and policies.
DR8	Interoperability	The architecture should expose standard interfaces between biometric services, examination systems, identity services and ledger components.
DR9	Human-centred trust	Security controls should be accompanied by transparency, privacy assurance, usability and stakeholder communication.
DR10	Dual evaluation	Technical performance and behavioural/organisational outcomes should both be evaluated.
DR11	Lifecycle privacy	Collection, processing, storage, access, retention, revocation and deletion must be governed across the biometric data lifecycle.

VII. PRIVACY-PRESERVING ARCHITECTURAL PRINCIPLES

A. Data Classification

Data type	Recommended location	Reason
Raw facial image	Controlled off-chain storage or local processing	High sensitivity; unnecessary on-chain persistence
Fingerprint/voice sample	Controlled off-chain storage or local processing	Sensitive biometric information
Protected biometric template	Encrypted protected store	Requires confidentiality and revocability mechanisms
Matching score	Transient/controlled application layer	Sensitive authentication evidence
Authentication decision	Application/audit layer	Needed for workflow and accountability

Cryptographic hash/event reference	Permissioned ledger	Provides integrity evidence
Timestamp/transaction metadata	Permissioned ledger	Supports auditability
Exam result	Authorised institutional record; hash/reference on ledger where appropriate	Balances confidentiality and integrity

B. Privacy Threat Model

Threat	Potential consequence	Control
Template theft	Irreversible biometric compromise	Template protection, encryption, key management
Ledger disclosure	Unnecessary exposure/linkability	Minimum metadata, pseudonymous identifiers
Insider misuse	Unauthorised access or secondary use	RBAC, separation of duties, audit logs
Cross-system correlation	Unwanted profiling	Domain-specific identifiers and controlled APIs
Excessive retention	Regulatory/privacy risk	Retention schedules and deletion workflows
Key compromise	Decryption or signing abuse	Secure key storage, rotation and revocation
Model bias/error	Unequal false decisions	Dataset diversity, subgroup evaluation and human review
Replay/presentation attack	False authentication	Liveness/PAD and challenge-response controls

The central privacy principle is architectural separation: the blockchain should provide durable evidence of event integrity without becoming the repository for raw or reconstructable biometric information.

Where stronger cryptographic privacy is required, future work may evaluate protected biometric matching, commitments, zero-knowledge mechanisms or other privacy-enhancing technologies, but their computational and governance costs must be evaluated rather than assumed to be negligible.

VIII. TECHNICAL DESIGN AND EVALUATION AGENDA

A. Biometric Fusion

The technical architecture should benchmark unimodal baselines against multimodal fusion under equivalent conditions. For each modality, report genuine and impostor score distributions and calculate FAR, FRR and EER under predefined thresholds. Score normalisation should be documented because heterogeneous modalities produce scores with different distributions.

Fusion weights should be justified using training/validation procedures rather than tuned on the final evaluation set.

B. Blockchain Performance

Blockchain evaluation should distinguish transaction confirmation latency from end-to-end authentication latency. Throughput should be reported as successfully committed transactions per unit time under defined concurrency. Permissioned-network benchmarks should report node count, consensus configuration, transaction payload size, hardware/software environment, network conditions and workload. This prevents claims about scalability that cannot be reproduced.

C. Baseline and Attribution

Future artefact evaluation should include at least three conditions: a conventional credential baseline, a unimodal biometric condition, and the proposed multimodal-plus-ledger condition. The baseline comparison permits attribution of gains to the proposed design. A factorial design can further separate the effects of multimodal authentication and blockchain logging.

Condition	Purpose
Credential-only baseline	Establishes conventional authentication reference
Unimodal biometric	Measures contribution of biometric verification
Multimodal biometric	Measures contribution of multimodal fusion
Multimodal + permissioned blockchain	Measures integrated security/integrity architecture
Privacy-preserving integrated condition	Measures privacy mechanism overhead where implemented

IX. ISDT-ORIENTED RESEARCH AGENDA

Following Gregor and Jones, the review-derived knowledge can be organised into an ISDT development pathway.

ISDT component	Proposed content
Purpose and scope	Secure, trustworthy and privacy-preserving e-examination authentication and auditability
Constructs	Identity assurance, multimodal fusion, privacy-preserving storage, blockchain auditability, trust, usability
Principles of form/function	Multimodal verification + privacy-preserving data separation + permissioned event anchoring
Artefact mutability	Modality set, fusion method, ledger platform and institutional governance may vary by context
Testable propositions	Improved identity assurance, auditability, and trust subject to privacy/usability constraints
Justificatory knowledge	Security principles, blockchain trust/integrity, biometric fusion, UTAUT and ISDT
Implementation principles	Least privilege, data minimisation, off-chain biometrics, secure APIs, permissioned governance
Expository instantiation	Functional prototype and evaluated deployment scenario

The review establishes purpose and scope, constructs and preliminary principles. The subsequent DSR study

must refine principles of form and function, define artefact mutability, formulate testable propositions, document implementation principles, and provide an expository instantiation.

A. Testable Propositions for Subsequent DSR

P1: Multimodal biometric authentication will provide lower identity-decision error than a unimodal biometric baseline under equivalent operating conditions.

P2: Adding a permissioned blockchain audit layer will increase verifiability and tamper evidence of authentication events without independently improving the correctness of the underlying biometric decision.

P3: Privacy-preserving data separation will reduce unnecessary exposure of biometric information relative to architectures that persist biometric data on shared ledgers.

P4: The integrated architecture will introduce measurable computational and transaction overhead; therefore, security gains must be evaluated jointly with latency and scalability.

P5: Perceived trustworthiness will depend on the joint effects of security performance, privacy assurance, transparency and usability rather than cryptographic integrity alone.

Figure 6. ISDT-Oriented Design Research Model

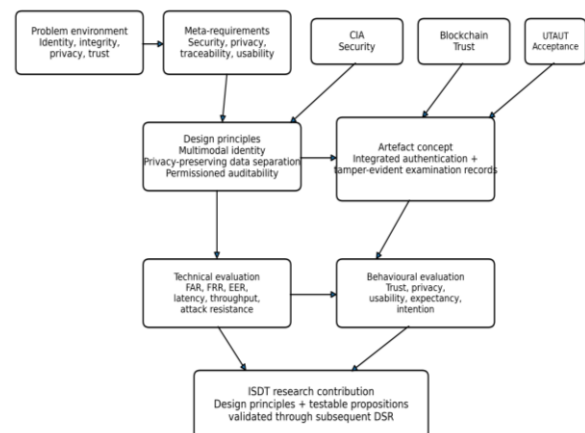


Fig. 6. ISDT-oriented design model connecting the problem environment, justificatory knowledge, design principles, artefact and subsequent evaluation.

Figure 7. Evidence-Emphasis Matrix Derived from the Literature Synthesis

	Identity	Integrity	Privacy	Trust	Governance	IS design
Biometrics	Strong	Limited	Moderate	Moderate	Limited	Limited
Blockchain	Limited	Strong	Mixed	Strong	Moderate	Limited
Integrated systems	Strong	Strong	Mixed	Limited	Limited	Limited
E-examination	Moderate	Moderate	Strong	Mixed	Moderate	Limited

Qualitative synthesis labels: Strong = repeatedly addressed; Moderate = recurring but incomplete; Mixed = conflicting/heterogeneous; Limited = comparatively underdeveloped.

Fig. 7. Qualitative evidence-emphasis matrix. The labels summaries the conceptual synthesis and are not fabricated study frequencies.

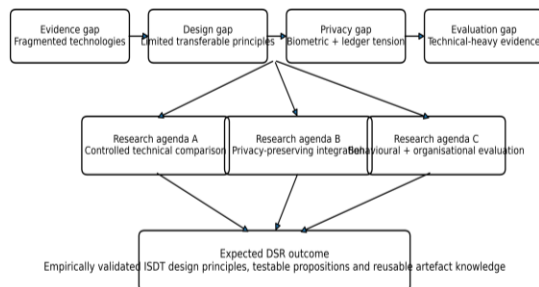
Figure 8. ISDT-Oriented Research Agenda Emerging from the Evidence

Fig. 8. ISDT-oriented research agenda linking review-derived gaps to subsequent Design Science Research.

X. DISCUSSION

A. Why Integration Matters

The review suggests that blockchain and biometrics should not be evaluated as competing authentication technologies. They operate at different points in the security lifecycle. Biometrics produces evidence about identity; blockchain produces durable evidence about recorded transactions. Their integration is therefore meaningful only when the architecture preserves the boundary between identity data and audit data.

B. Why Privacy Must Be an Architectural Property

Privacy cannot be added after system implementation. The architecture determines what data are collected, where they are processed, how long they persist, who can access them, and what becomes immutable. The review therefore treats privacy-preserving data separation, minimisation and lifecycle governance as design requirements rather than compliance add-ons.

C. Why Technical Accuracy Is Insufficient

A system can achieve low biometric error rates while remaining organisationally unacceptable if it is intrusive, opaque, difficult to use or poorly governed. Conversely, an immutable ledger can preserve records accurately without preventing a fraudulent event from being accepted. Trustworthiness is therefore a composite socio-technical outcome requiring technical, behavioural and governance evidence.

D. Implications for Resource-Constrained Institutions

Integrated security architectures should account for bandwidth, device availability, compute capacity, biometric sensor quality, network reliability and technical support. A theoretically secure architecture that cannot operate reliably under institutional constraints may reduce rather than improve trust. Future evaluation should therefore include realistic concurrent workloads and deployment contexts, including institutions where infrastructure is heterogeneous.

XI. LIMITATIONS AND EVIDENCE-INTEGRITY BOUNDARIES

This manuscript intentionally separates review methodology from verified empirical review results. The attached working paper did not contain a verified database export, deduplicated screening log, full-text exclusion log, or completed study-extraction matrix. Consequently, this rebuilt version does not invent PRISMA counts, annual publication frequencies, percentages, or study-level performance values. Before journal submission as a completed SLR, the protocol must be executed against the named databases, the screening and extraction records must be archived, and all quantitative figures must be generated from that evidence. Second, database coverage can still introduce indexing bias; citation chaining and multiple databases reduce but do not eliminate this risk.

Third, heterogeneity in biometric datasets, blockchain architectures and evaluation metrics may make statistical meta-analysis inappropriate. Fourth, publication bias and selective reporting may affect the evidence base. Fifth, the proposed design requirements remain review-derived until empirically validated through DSR.

XII. CONCLUSION

Secure e-examination is best understood as an Information Systems design problem involving identity assurance, information integrity, privacy, trust, governance and usability. The systematic-review framework developed in this paper addresses major weaknesses identified in the earlier manuscript by separating the evidence streams, specifying reproducible search procedures, defining explicit eligibility and appraisal criteria, structuring extraction variables, and distinguishing descriptive synthesis from thematic and design-oriented interpretation.

The conceptual synthesis indicates that multimodal biometrics and permissioned blockchain are complementary rather than substitutive technologies. Multimodal biometrics strengthens candidate identity assurance, while blockchain can provide tamper-evident and auditable evidence about authentication and examination events. Their integration nevertheless introduces a critical privacy tension because biometric information is sensitive and difficult to revoke whereas blockchain records are intentionally persistent.

The paper consequently derives a bounded set of review-oriented design requirements centred on multimodal identity assurance, transparent fusion, presentation-attack resistance, privacy-preserving data separation, tamper-evident logging, permissioned governance, interoperability, human-centred trust, lifecycle privacy and dual technical-behavioural evaluation. These requirements are not claimed as validated ISDT principles. Rather, they constitute a theoretically grounded starting point for Design Science Research.

The next empirical stage should instantiate these requirements, compare the proposed architecture with credential and unimodal baselines, evaluate technical and behavioural outcomes, and use the results to refine testable propositions and reusable design principles. In this form, the review provides a defensible bridge between fragmented technology literature and a cumulative Information Systems research programme for secure, trustworthy and privacy-preserving digital assessment.

REFERENCES

- [1] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, Art. no. n71, 2021, doi: 10.1136/bmj. n71.
- [2] M. L. Rethlefsen et al., "PRISMA-S: An extension to the PRISMA statement for reporting literature searches in systematic reviews," *Systematic Reviews*, vol. 10, Art. no. 39, 2021, doi: 10.1186/s13643-020-01542-z.
- [3] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004, doi: 10.2307/25148625.
- [4] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007, doi: 10.2753/MIS0742-1222240302.
- [5] D. Jones and S. Gregor, "The anatomy of a design theory," *Journal of the Association for Information Systems*, vol. 8, no. 5, 2007, doi: 10.17705/1jais.00129.
- [6] S. Gregor and A. R. Hevner, "Positioning and presenting design science research for maximum impact," *MIS Quarterly*, vol. 37, no. 2, pp. 337–355, 2013, doi: 10.25300/MISQ/2013/37.2.01.
- [7] A. Alammery, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-based applications in education: A systematic review," *Applied Sciences*, vol. 9, no. 12, Art. no. 2400, 2019, doi: 10.3390/app9122400.
- [8] C. Delgado-von-Eitzen, L. Anido-Rifón, and M. J. Fernández-Iglesias, "Blockchain applications in education: A systematic literature review," *Applied Sciences*, vol. 11, no. 24, Art. no. 11811, 2021, doi: 10.3390/app112411811.
- [9] P. Ocheja, F. J. Agbo, S. S. Oyelere, B. Flanagan, and H. Ogata, "Blockchain in education: A systematic review and practical case studies," *IEEE Access*, vol. 10, pp. 99525–99540, 2022, doi: 10.1109/ACCESS.2022.3206791.
- [10] Z. H. Goh, Y. Wang, L. Leng, S.-N. Liang, Z. Jin, Y.-L. Lai, and X. Wang, "A framework for multimodal biometric authentication systems with template protection," *IEEE Access*, vol. 10,

- pp. 96388–96402, 2022, doi: 10.1109/ACCESS.2022.3205413.
- [11] M. Abdul-Al, G. Kumi Kyeremeh, R. Qahwaji, N. T. Ali, and R. A. Abd-Alhameed, “The evolution of biometric authentication: A deep dive into multi-modal facial recognition: A review case study,” *IEEE Access*, vol. 12, 2024, doi: 10.1109/ACCESS.2024.3486552.
- [12] F. J. de Haro-Olmo, Á. J. Varela-Vaca, and J. A. Álvarez-Bermejo, “Blockchain from the perspective of privacy and anonymisation: A systematic literature review,” *Sensors*, vol. 20, no. 24, Art. no. 7171, 2020, doi: 10.3390/s20247171.
- [13] S. Han, S. Nikou, and W. Y. Ayele, “Digital proctoring in higher education: A systematic literature review,” *International Journal of Educational Management*, vol. 38, no. 1, pp. 265–285, 2024, doi: 10.1108/IJEM-12-2022-0522.
- [14] D. G. Balash, D. Kim, D. Shaibekova, R. A. Fainchtein, M. Sherr, and A. D. Aviv, “Examining the examiners: Students’ privacy and security perceptions of online proctoring services,” *arXiv preprint arXiv:2106.05917*, 2021.
- [15] D. G. Balash, R. A. Fainchtein, E. Korkes, M. Grant, M. Sherr, and A. D. Aviv, “Educators’ perspectives of using (or not using) online exam proctoring,” *arXiv preprint arXiv:2302.12936*, 2023.
- [16] N. Abo Alzahab, G. Rafaiani, M. Battaglioni, F. Chiaraluce, and M. Baldi, “Decentralized biometric authentication based on fuzzy commitments and blockchain,” *arXiv preprint arXiv:2409.11303*, 2024.
- [17] J. Lai, T. Wang, S. Zhang, Q. Yang, and S. C. Liew, “BioZero: An efficient and privacy-preserving decentralized biometric authentication protocol on open blockchain,” *arXiv preprint arXiv:2409.17509*, 2024.